Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

020.205 IT System Technical Assessments

Version 2.1
December 15, 2017

Revision History

Date	Version	Description	Author
5/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
12/15/2017	2.1	Revision Date	CHFS OATS Policy Charter Team
12/15/2017	2.1	Review Date	CHFS OATS Policy Charter Team

Sign-Off

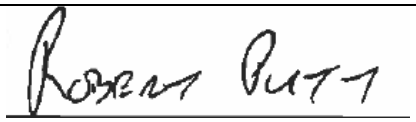
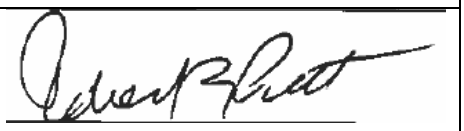
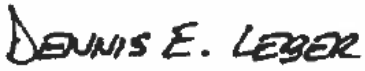
Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	12/15/2017		
CHFS Chief Security Officer (or designee)	12/15/2017		

Table of Contents

020.205 IT System Technical Assessments

Category: 020.200 Managerial Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a system technical assessment policy. This document establishes the agency's Information Technology (IT) System Technical Assessments to manage risks and provide guidelines for security best practices regarding the agency's IT assessments.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

This policy applies to all systems and/or applications implemented subsequent to the 2017 policy review/revision date. Systems and/or applications implemented prior to the 2017 policy review/revision will be considered for compliance with this policy based upon consideration of priority, resources, and funding availability.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the CHFS OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3 Policy Requirements

3.1 General

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) Enterprise CIO-082 Critical Systems Vulnerability Assessments Policy. CHFS OATS works collaboratively with program areas to determine the level of sensitivity for its data.

The CHFS executive leadership along with business partners and other stakeholders shall define the agency's critical systems that are subject to meet the assessments listed and defined within this policy. Although not mandatory, all other agency systems containing sensitive data, but not deemed critical, may also comply with IT Technical assessment requirements outlined in this policy.

CHFS utilizes the NIST federal standards as well as FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems for determining its critical systems. Utilizing FIPS 199, a system is defined as critical when the potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Per Enterprise CIO-082 Policy, for those systems deemed critical, the CHFS is responsible for engaging a third party to assist in conducting vulnerability assessments both upon implementation into production and every two (2) years thereafter.

CHFS also follows 065.014 CHFS Software Development Lifecycle (SDLC) and New Application Development Policy and CHFS 040.201 Internal Risk Assessment Policy. Vulnerability assessments may be performed by internal CHFS OATS IS Team or contracted to approved third party assessment providers as approved by the Office of the Secretary IT Executive, CHFS CISO, or designee.

3.2 Security IT Staff Responsibility

CHFS OATS IS Team is responsible for oversight of vulnerability assessments of each system covered by this policy. If the agency decides to use a third party vendor, the CHFS IS Team is responsible to ensure the third party vendor is qualified and approved by appropriate CHFS management. The CHFS OATS IS Team is responsible for updating this policy, as well as associated procedures when changes to the infrastructure or enterprise environment occur.

3.3 Assessments Details

CHFS OATS IS Team utilizes a layered approach methodology to application security testing. The methodology for this assessment includes: Discovery, Vulnerability Scanning, Manual Penetration Testing, Vulnerability Assessments, and Security Reviews.

4 Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Critical Systems:** any system or application that is federally mandated/regulated will be defined as a critical system. For all other systems/applications classification shall be determined through a Business Impact Assessment (BIA). CHFS ITMP will be the source of knowledge and repository of severity level for systems/applications.
- **Discovery:** Manually walking through the web application to understand the logic and operational flows in order to filter out information that may generate messages or email triggered by scanning.
- **Manual Penetration Test:** Examine specific flaw categories that currently require manual inspection to evaluate the security of the infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations, or risky end-user behavior.
- **Security Review:** The security assessment will end with a list of all vulnerabilities that are found through the web. Risk should be prioritized based on the ease of exploiting the vulnerability and the potential harm that could result if an attacker is successful. The results will be disseminated to the project team, who will then prioritize what needs to be fixed so that existing applications can be hardened. Those applications being built can be remedied and safely placed into production.

- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **Vulnerability Assessment:** Results from the automated and manual testing are combined to deliver a consolidated assessment report to simplify the remediation process.
- **Vulnerability Scan:** Execute the automated assessment tools to perform the diagnostic phase of a vulnerability analysis. Vulnerability analysis defines, identifies, and classifies the lapse in security (vulnerabilities) in a web application. The automated vulnerability scan is non-intrusive.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 040.201 Internal Risk Assessment Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: Risk Assessment Program Procedure
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessments Policy
- Internal Revenue Services (IRS) Publication 1075

- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- National Institute of Standards and Technology (NIST) Special Publication 800-12 Revision 1, Introduction to Information Security (Draft)
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information